

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

EB Docket No. 06-36

ANNUAL 47 C.F.R § 64.2009(e) CPNI CERTIFICATION

Annual 64.2009(e) CPNI Certification for 2008

Date filed:

February 23, 2009

Name of company covered by this certification: **Bluemile, Inc.**

Form 499 Filer ID: **826470**

Name of signatory: **Thomas J. Busic, Jr.**

Title of signatory: **Chief Executive Officer**

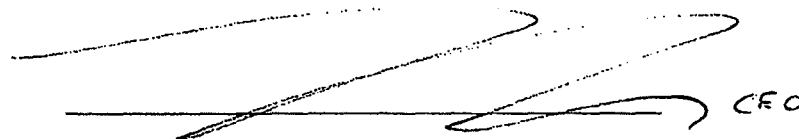
I, Thomas J. Busic, Jr., certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules, to the extent those procedures apply to the information we obtain from our carrier customers. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system or at the Commission) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



CEO

BLUEMILE, INC.
STATEMENT OF CPNI PROCEDURES

Bluemile, Inc. ("Bluemile") takes the protection of CPNI seriously. Bluemile has received legal counsel in this area and protects the confidentiality of its carrier customers' information. Bluemile receives limited information from its carrier customers and uses that information solely to perform the telecommunications services, for billing purposes and in response to legal process. It does not use this information for marketing purposes.

Duty to Protect CPNI

We recognize that communications companies have a duty to protect customer CPNI. Carriers may not disclose CPNI to unauthorized persons, nor may carriers use CPNI in certain ways without customer consent. Before carriers can provide customers with their own CPNI, they must authenticate the customer.

There are a few cases in which carriers can disclose CPNI without first obtaining customer approval:

1. **Administrative use:** Carriers may use CPNI to *initiate, render, bill and collect* for communications services.
2. **Protection of carrier and third parties:** Carriers may use CPNI to protect their interests, such as to prevent fraud or illegal use of the carriers' systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.
3. **As required by law:** Carriers may disclose CPNI if required by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Again, employees are notified of any steps they must take in these situations.

As described more fully below, given the nature of Bluemile's wholesale business, most or all of our disclosure of CPNI falls under the administrative use exception outlined above. Therefore, the customer notification, approval, and authentication requirements set forth by the FCC do not apply to our business.

Our Own Use Of CPNI

At this time, we do not use CPNI to market to our carrier customers. However, at a later date, we may use CPNI to provide or market services to our existing customers. We understand that we are required to obtain customer approval prior to using CPNI in certain ways, and will ensure compliance if we seek to use CPNI to market services.

We do not share CPNI with any affiliates or other third parties for marketing purposes.

We regularly review our marketing practices to determine if and how CPNI is used within the company, and whether CPNI is being shared with other entities. We also review new marketing or sales campaigns to ensure compliance with the FCC's CPNI regulations.

Authenticating Customers Before Disclosing CPNI

We understand that carriers are required to authenticate customers before disclosing CPNI to them. The type of authentication required varies based on the customer's method of communicating with the carrier: by telephone, in person, by mail, or online.

We only disclose CPNI to third-party vendors to manage trouble tickets or bill and collect for telecommunications services rendered. Our third-party billing vendor uses the CPNI disclosed by Bluemile to prepare invoices and post the invoices on a secure FTP website which may only be accessed by customers using a unique user name and password. No one may obtain CPNI from our vendors by any other means.

We do not provide CPNI directly to our wholesale customers. Although we do not currently disclose CPNI to our customers, if this policy should change, we will train our employees regarding the authentication procedures that must be followed before providing CPNI to customers.

Training And Discipline

We train all of our employees regarding our CPNI policies on an annual basis to ensure that they understand Bluemile's CPNI policies and any updates to those policies. New employees who will have access to CPNI are trained when they join the company, and then attend the regularly-scheduled retraining sessions. Employees are subject to disciplinary action for failure to abide by our requirements.

Record-Keeping

We maintain the following records for two (2) years:

- a. Employee disciplinary records; and
- b. Records of discovered CPNI breaches, notifications to law enforcement regarding breaches, and any responses from law enforcement regarding those breaches.

These records are maintained electronically on a secure server for the time required, then deleted. If the records are paper records, they are converted to electronic format for storage, and the paper records are destroyed.

Notification Of Account Changes

We understand that we are required to notify customers when changes have been made to authentication passwords, customer responses to back-up means of authentication, online accounts, or addresses of record by mailing a notification to the account address of record. We do not reveal the changed account data in the notification.

Unauthorized Disclosure Of CPNI

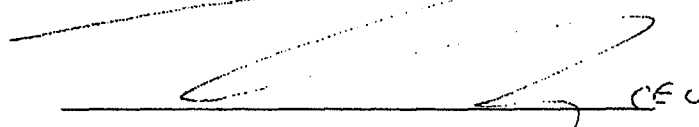
We understand that we must report CPNI breaches to law enforcement no later than seven (7) business days after determining the breach has occurred, by sending electronic notification through the link at <http://www.fcc.gov/eb/CPNI/> to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). Mark DiGiovanni, our CPNI Compliance Officer, is responsible for this notification.

We understand that we may not notify customers or the public of the breach earlier than seven (7) days after we have notified law enforcement through the central reporting facility. If we wish to notify customers or the public immediately, where we feel that there is "an extraordinarily urgent need to notify" to avoid "immediate and irreparable harm," we inform law enforcement of our desire to notify and comply with law enforcement's directions.

Records relating to such notifications are kept in accordance with our record-keeping policies. These records include: (i) the date we discovered the breach, (ii) the date we notified law enforcement, (iii) a detailed description of the CPNI breached, and (iv) the circumstances of the breach.

During the course of the year, we compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. We include this information in our annual CPNI compliance certification filed with the FCC.

Signed

A handwritten signature in dark ink, appearing to read "Mark DiGiovanni", is written over a horizontal line. To the right of the signature, the initials "CEU" are handwritten.